Abstract: The BGP TTL Security Hack <draft-gill-btsh-01.txt>

Dave Meyer, Sprint
Draft authors: Vijay Gill, John Heasly, and Dave Meyer

In recent weeks and months, we have been seeing a large number of DoS attacks directed against port 179 (BGP). These attacks are enabled in part by the facts that (i). the TCP 4 tuple is easy to discover, and (ii). the attack doesn't require knowledge of the TCP sequence number. As a result, you don't have to directly compromise ("own") the attacked router to disable BGP processing.

The BGP TTL Security Hack (BTSH) is designed to protect the BGP (RFC1771) infrastructure from CPU-utilization based attacks. While BTSH is most effective in protecting directly connected BGP peers, it can also provide a lower level of protection to multi-hop sessions.

About the Presenter
David Meyer is currently Senior Scientist and Director of IP Technology Development at Sprint. He is also Director of the Advanced Network Technology Center at the University of Oregon. Prior to working at Sprint, Dave worked at Cisco, where he was involved in software development, working both on multicast and BGP. He is active in the IETF, where he chairs the MBONED and MSDP (Multicast Source Discovery Protocol) working groups, as well as being a member of several IETF directorates and IRTF research groups. Dave is a longtime member of the operator community, and is a member of the NANOG program committee. He is also active in other standards organizations, such as ANSI T1X1.

PDF presentation
RealVideo stream

Merit Network, Inc.
4251 Plymouth Road Suite 2000
Ann Arbor, MI 48105-2785
734-764-9430